TECH INDUSTRY

Bitcoin takes a hit as China bans cryptocurrency offerings

The country says there have been too many scams resulting from initial coin offerings, and it's putting a stop to that.

BY **ZOEY CHONG** / SEPTEMBER 4, 2017 9:19 PM PDT

China has a new target on its internet hit list: cryptocurrency.

Bitcoin

Science Picture Co

The People's Bank of China banned initial coin offerings -- raising funds by launching new digital tokens -- following a series of investigations, it announced Monday. There was no mention of cryptocurrencies such as Bitcoin or its rival Ethereum, but the announcement sent stocks sliding anyway.

The burgeoning market for cryptocurrencies, which has grown so quickly that one bitcoin was worth more than an ounce of gold in March, has seen digital currency entrepreneurs flocking to ICOs to create and sell digital tokens to investors, who include celebs such as Paris Hilton.

MORE READS

Bitcoin soars to record high following cryptocurrency split

You can't buy much online with bitcoin, says report

Bitcoin value plummets after hackers steal millions from exchange

Still, regulators are not taking to ICOs well. The practice, which Bloomberg said netted $1.6 billion in the last year, has prompted security concerns from the US Securities and Exchange Commission. The Commission released advisories in July and August saying some ICOs should be regulated like other securities, warning of risks that come with investing in ICOs, including scams.

ICOs are a form of "unauthorised and illegal public financing," the People's Bank of China said in a statement, adding that ICOs have "seriously disrupted economic and financial order" in China.

The People's Bank said the country has banned all sales and currency conversions involving digital tokens, and prohibited all financial institutions and non-bank payment organisations from offering any services to ICOs.

Tech Enabled: CNET chronicles tech's role in providing new kinds of accessibility.

Batteries Not Included: The CNET team reminds us why tech is cool.

SHARE YOUR VOICE

4 comments

TAGS

Tech Industry

Bitcoin

Next Article: Homeland Security's tall order: A hacker-free election

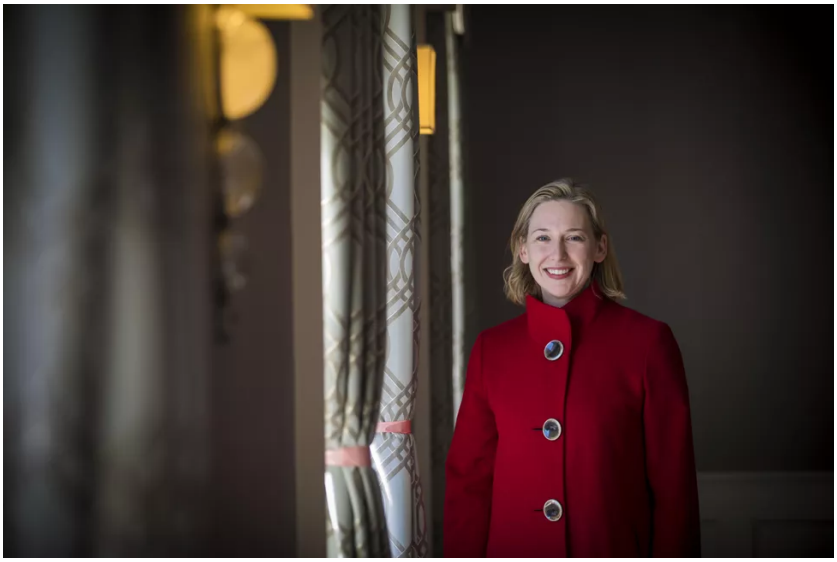
SECURITY

Homeland Security's tall order: A hacker-free election

Jeanette Manfra, the top cybersecurity official at DHS, tells CNET about all the ways hackers can

sow chaos in this year's primaries and midterm elections.

BY **LAURA HAUTALA** / FEBRUARY 23, 2018
4:00 AM PST



James Martin/CNET

As lawmakers and federal investigators continue to try to understand the chaos foreign actors were able to create during the 2016 election, the US Department of Homeland Security has taken a central role in helping secure the next election.

The agency declared the US election system, which is run by a fragmented group of officials in all 50 states as well as dozens of smaller local governments, to be a part of the nation's "critical infrastructure" in January 2017. The agency doesn't have any legal authority over election officials, but it offers programs to help them keep hackers out of voting machines, voter registration databases and public-facing election websites.

Homeland Security's top cybersecurity official, Jeanette Manfra, sat down with CNET to talk about the balancing act of helping secure elections without overstepping the federal government's authority. She serves as the National Protection and Programs Directorate Assistant Secretary for the Office of Cybersecurity and Communications at Homeland Security. Manfra told us that, so far, 32 states and 31 local governments have taken part in at least the most basic cybersecurity help offered by Homeland Security, and the agency will have finished 14 deeper assessments by the end of April.

What's more, Manfra said Homeland Security hasn't seen a concerted hacking effort targeting the election system like it saw in 2016 -- so far.

"The intelligence community has said we have every reason to expect that this foreign influence activity will continue, but we don't see any specific credible threat or targeting of election infrastructure," Manfra said.

Manfra also talked with us about why she thinks a return to paper ballots wouldn't create a totally secure election, what Homeland Security has done to secure the federal government since the disastrous Office of Personnel Management data breach in 2015, and how she thinks the government can help make the internet of things safer. Here's an edited transcript of our conversation.

Q: Tell us what Homeland Security is doing to help states and local governments secure the vote.
Manfra: When the government has information that would be useful to election officials, that we get that to them.

We issued a few public statements over the past couple of days about a series of meetings with industry, with state and local government officials. If there's somebody targeting a network or a system in your state, who are the people that we need to notify.

To the extent that they would like to take advantage of the services we have, we offer those as well. There's everything from scanning -- they provide us with their IP ranges, we provide them with a weekly report on any vulnerabilities that we identify.

The other one that's been written about a lot is the risk and vulnerability assessment. It takes about three weeks. They lay out for us what their networks, what their systems look like. We try a variety of different things and identify where we saw some potential issues, some recommended mitigations, and we often times will talk through with them if they have any questions.

Can you speak to the difference between securing voting machines and securing voter rolls and other election related networks?
Manfra: The voting machines tend to make a lot of news when you've got people talking about being able to hack into them. While technically somebody may be able to demonstrate it, it's nearly impossible to gain physical access to those machines.

Then you've got all these other pieces of the system, where if somebody wanted to [they could] create confusion. It's got nothing to do with actually changing a vote, but you try to get into

these different systems, because people don't understand necessarily how all of these pieces are very disconnected.


A voter during the 2016 US presidential election.

A voter during the 2016 US presidential election.
Brianna Soukup/Getty Images

We published voter registration database best practices in 2016. We've been working with software vendors. We've been working with state officials. How can they best ensure that their public-facing websites are protected? How can they ensure that there's no disruption of voter rolls? We're working with the different organizations that would publish [early results], whether that's through a state site, or the AP.

Not that we're seeing targeting of any of this. We're just wanting to take a really comprehensive approach to what we consider election infrastructure. Because it's virtually impossible to actually affect the vote count itself, then an adversary may want to look at other means.

Security experts have been warning that voting machines are vulnerable to hacks for years, even if they would have to be hacked in person. What's your approach with the vendors of these machines in ensuring that this improves?
Manfra: My approach with the vendor community is more nascent. We had a meeting with them last Thursday, and have had some individual meetings, and we've got our own team of experts to look and do some penetration testing. I would say it's a little bit early for me to judge them, and pretty much anything is going to have some vulnerability that somebody is going to try to exploit.

I also believe that once you have a product, you also have to make sure that you're doing everything you can to lower the risk. It's not always a cyberfix for a cybervulnerability; sometimes it's reducing physical access, like they've done, and there's other mechanisms in place such as the transparency of our election process. We've got observers that are looking at the vote counts and would be able to identify if there's any anomalous changes.

I've talked to some advocates who say we should move back to paper ballots across the board. Would that make things more secure?
Manfra: I vote in a community who's gone to paper ballots. That introduces different complexity that those digital machines were trying to overcome. I couldn't say that that will just unilaterally remove all risk. Particularly because if you have an adversary

whose goal is to just create confusion, and undermine confidence, it wouldn't necessarily matter.

I do believe that there should be audit capability and redundant means for checking if there is suspicion that something happened. And I know a lot of states and localities already have it, and if they didn't, they're working on it.

If there's no current signs of foreign activity against US election systems, that's different from what you've said was seen in the 2016 election when 21 states were targeted and a few were actually -- is breached the right word?
Manfra: That's been the subject of endless debates.

But now you're saying you're not seeing a specific, concerted efforts along those lines...
Manfra: ...targeting election systems at this time. But again, what the intelligence officials laid out is, there is no reason to believe that the previous activity would go away.

There was an initial announcement that elections would be considered critical infrastructure because there was concerns over federal involvement in the state and local processes. Can you speak to where those concerns are coming from and how you deal with the challenge of offering assistance in elections that Homeland Security doesn't have authority over?
Manfra: In our non-federal cybersecurity role, we've tried to focus on what are those critical services and functions that we depend upon. Access to clean water, electricity and communications, and confidence in the financial systems. We have no kind of oversight or directive authority over any of those functions. Some of them may be regulated by other parts of the state government or the federal government, but not by us. And we think that [Homeland Security's] voluntary approaches have been very useful.

> “Pretty much anything is going to have some vulnerability that somebody is going to try to exploit."
>
> Jeanette Manfra, DHS

Not every state is using every service offered by Homeland Security. What are some of the reasons a state might not opt into some of this?
Manfra: We have a lot of great partnerships with organizations across the country that never take any of our services because they're buying their own. If they'd like to take advantage [of ours], then that's great. It benefits both of us. We learn about their systems, and they're able to participate in our programs for free.

What has changed in the government's approach to securing federal networks since the Office of Personnel Management breach in June of 2015?
Manfra: That was only three years ago, [but] it feels like a lifetime. At Homeland Security, Congress has given us a lot of authority. [We've been] implementing those authorities, many of them we got in 2014 and 2015. The binding operational directive is one that we've been using successfully. You saw in the president's executive order [in May 2017] very clearly that cabinet secretaries, heads of agencies, you are accountable for your cybersecurity. This needs to be a priority for you.

The first directive we issued was about patching critical vulnerabilities within 30 days. We were not there when that started. And we're now largely in that [range].

How developed is the information sharing system authorized under the Cybersecurity Information Sharing Act in 2015, and what has Homeland Security been able to do with it so far?
Manfra: For the automated indicator sharing -- remembering that it's all about volume and velocity, and not about human validation for every single indicator -- we've shared 1.8 million unique indicators through that program. We've got a little over 200 organizations that are signed up for it.

Are those private and public sector organizations?
Manfra: Yes. And the 200 doesn't necessarily mean a company or an agency. We've got a lot of information sharing organizations that have thousands of customers.

In 2016 we saw internet of things devices being used in unprecedented DDOS attacks. Now we're seeing botnets, including IoT botnets, caught up in cryptojacking schemes. What do you see Homeland Security's role in setting security standards for the growing network of sensors in our homes, workplaces and industrial settings?
Manfra: In traditional consumer products, you can look at your microwave and see the UL seal there and you know that it's

passed some level of standards and certification. I think that is probably what we need for the so-called internet of things.

What we've looked at is Underwriter Laboratories, Energy Star and different things that have now become an industry standard -- how did they develop? I think that there's a government role in nurturing that process, but not dictating what the standards are. I think at one point the government said we're only going to buy Energy Star products, and that was a very clear indicator for the market. I'm not suggesting that we have any plans along those lines, but I think it's worthwhile looking back at how some of these different certification programs came about. I want to keep seeing the innovation, but I also want to see some standards.

When it comes to critical infrastructure like power plants and water systems, we've only seen small attacks in the US, such as the breach of a control system for a small dam in Rye Brook, NY. But places like Ukraine have seen problems like power outages. What's your assessment of the threat to the US electrical grid and other physical infrastructure?
Manfra: I think the advantage that the US has in a lot of its critical infrastructure is it's not very connected yet. A lot of it is very legacy systems. When you're talking about water systems, you have some large water systems in our country, but it's still very local. The electric grid has a long history of resilience.

What we're working with with all the different industries is to recognize what we've done to build resilient systems for natural hazards or terrorist attacks, and all these different things that people have been working on now for quite a long time, [and asking,] how can we use those processes to manage a cyber incident, and where is there potentially a difference?

iHate: CNET looks at how intolerance is taking over the internet.

Blockchain Decoded: CNET looks at the tech powering bitcoin -- and soon, too, a myriad of services that will change your life.

SHARE YOUR VOICE

13 comments

TAGS

Security | Smart Home | Hacking | Government surveillance

Next Article: 'Annihilation' director wove memory into